AFFAIRE « LAFARGE »
LES MOYENS D'ENQUÊTE UTILISÉS ET QUELQUES ATTENTIONS À EN TIRER



Brochure éditée par des soutiens des personnes mises en cause dans l'affaire « Lafarge ».

Septembre 2023

- Conseils sur l'obligation de donner son code de téléphone : https://paris-luttes.info/du-nouveau-sur-l-obligation-de-15018?lang=fr

- Fadettes, UFED et données de connexion : les techniques d'investigation numériques de la police : https://paris-luttes.info/fadettes-ufed-et-donnees-de-16236?lang=fr

Sur la garde-à-vue en particulier :

- Petit manuel de défense collective de la rue au tribunal, brochure : https://infokiosques.net/spip.php?article1788

- En GAV, je n'ai rien à déclarer, petite BD : https://infokiosques.net/spip.php?article1863

- Comment la police interroge et comment s'en protéger, livre : https://projet-evasions.org/wp-content/uploads/2022/07/220707PDF-fr-web-interro.pdf

Sur le fichage et les procédures d'effacement :

- Sur la "nouvelle" possibilité de prise de force des empreintes digitales : https://www.laquadrature.net/2023/05/12/en-gav-tes-fiche%c2%b7e-episode-2-les-empreintes/

- Sur les procédures d'effacement, avec des lettres-types : La folle volonté de tout contrôler : https://rebellyon.info/IMG/pdf/fichiers_police_justice_renseignement_v3_novembre_2021.cleaned.pdf

Sur la répression d'autres affaires visant la gauche radicale :

- Les hiboux face à la justice : état des lieux de la répression à Bure (2019) : https://bureburebure.info/wp-content/uploads/2019/09/etat-des-lieux-de-la-repression-Bure-septembre-2019.pdf

- Les inculpés du 8 décembre : https://soutienauxinculpeesdu8decembre.noblogs.org/files/2023/05/brochure8.12pourimpression.pdf

- Le vélo et le feu, à propos de l'enquête qui vise Ivan pour incendie de voitures, menée par la SDAT : https://infokiosques.net/spip.php?article1973

Glossaire

Anacrim : Fichier de regroupement des affaires judiciaires
Fadettes : Factures détaillées
DGSI : Direction Générale de la Sécurité Intérieure
FAED : Fichier Automatisé des Empreintes Digitales
FNAEG : Fichier National Automatisé des Empreintes Génétiques
GAV : Garde-à-vue
IMEI : Numéro d'identification unique de la puce GSM (il permet d'identifier un téléphone)
IMSI : International mobile subscriber identity, identité internationale d'abonné.e mobile, numéro unique stocké dans la carte SIM
PNIJ : Plateforme nationale des interceptions judiciaires, elle permet d'obtenir en quelques clics les résultats de réquisitions liées à la téléphonie mobile
SDAT : Sous-direction antiterroriste
SR : section de recherche (de la gendarmerie)
TAJ : Traitement des Antécédents Judiciaires

Ressources

Sur le développement d'une culture et des pratiques de sécurité

- Comment se protéger et protéger nos luttes, premiers pas dans la mise en place de pratiques de sécurité : https://infokiosques.net/spip.php?page=lire&id_article=2017

- Confidence, Courage, Connection, Trust (en anglais) : https://north-shore.info/wp-content/uploads/2019/11/confidence-courage.pdf

Sur le numérique en général

- Guide d'autodéfense numérique https://guide.boum.org/

- TuTORiel Tails https://infokiosques.net/spip.php?article1726

Sur la téléphonie en particulier :

- Téléphonie mobile – surveillances, répressions, réduction des risques : https://infokiosques.net/spip.php?article1975

- Sur la demande de code de déverrouillage du téléphone en GAV : https://www.laquadrature.net/2023/04/28/en-gav-tes-fiche%c2%b7e/

Ce texte fait suite aux 35 arrestations des 5 et 20 juin dernier et en particulier aux 31 concernant le désarmement de l'usine Lafarge de Bouc-Bel-Air, le 10 décembre 2022.

Parmi ces personnes, deux ont été mises en examen début juillet. Les analyses qui suivent sont donc le résultat d'entretiens menés d'une part avec les arrêté.e.s qui ont pu faire part d'informations recueillies lors des auditions, dans leurs discussions avec les services d'enquête, d'autre part avec les mis.es en examen, chacun de leur côté, étant donné qu'iels ont interdiction d'entrer en contact.

Elles permettent de se faire une idée de ce que l'État est prêt à déployer pour traquer celleux qui s'opposent au ravage écologique et aux nuisances industrielles. Dans cette affaire, menée sur place par la section de recherche de la gendarmerie de Marseille, la SDAT (sous-direction antiterroriste, voir glossaire à la fin) a été saisie en renfort, alors même que les faits reprochés ne sont pas caractérisés comme terroristes et ce sur la base de la seule et vague notion de « violences extrêmes ». Les moyens à leur disposition sont considérables - téléphonie, écoute, filature, logiciel espion, reconnaissance faciale, balise GPS, etc.

Les moyens décrits ici ne reflètent pas la majorité des enquêtes sur des actions politiques. Certains moyens sont courants, d'autres beaucoup plus rares. Tous n'ont vraisemblablement pas été déployés à l'encontre de toutes les personnes visées dans l'affaire Lafarge, mais selon notre analyse de manière graduelle, suivant l'intérêt spécifique que semblait représenter telle ou telle personne pour leur enquête. L'ensemble de l'utilisation de tous ces outils est à notre connaissance encore relativement singulière, complexe, coûteuse et donc relativement rare.

Résister à la surveillance nous protège les un.es les autres. Nous aimerions que ces mauvaises expériences puissent servir à nourrir des pratiques et une culture commune de la sécurité, bien au-delà des personnes directement visées par cette enquête.

Organisation générale de l'enquête

La Section de Recherche de la gendarmerie de Marseille est semble-t-il mobilisée dès le soir du 10 décembre 2022. Il semblerait qu'à partir d'une première analyse des images de vidéosurveillance, des analyses des relevés d'ADN, d'empreintes et des bornages téléphoniques, une première liste de personnes suspectées d'avoir été présentes sur les lieux ait été rapidement créée.

La SDAT est co-saisie dans l'enquête. Elle se renseigne sur les sites/groupes qui ont évoqué l'action du 10 décembre, envoie des réquisitions à Twitter, Instagram ou Facebook pour obtenir des identités liées à ces sites et ces groupes. Au bout de 14 jours, durée maximum d'une enquête de flagrance, une enquête préliminaire est ouverte. Les objets devant être soumis à des prélèvements ADN sont envoyés à la police scientifique, analyse qui prend un certain temps. L'analyse des images de vidéosurveillance s'attèle à traiter des centaines d'heures de vidéos, et s'étend donc sur plusieurs mois.

Ainsi, selon ce qui nous est donné à comprendre, la première séquence de l'enquête qui se base essentiellement sur les recherches effectuées sur place (vidéosurveillance, analyse de la téléphonie sur les lieux et relevés ADN) s'achève avant l'ouverture de l'instruction judiciaire en date du 2 février.

Dans un second temps, ils ont cherché à déterminer un deuxième cercle de personnes (proches des suspect.es) en étudiant les "fadettes" (factures détaillées de téléphonie), les virements bancaires et ont parfois, mais pour un nombre restreint de personnes, déployé ou demandé de déployer des moyens de surveillance humaine (filatures) ou techniques (traceurs GPS, interceptions téléphoniques, logiciels espions).

Les données récoltées sur l'entourage des premières personnes soupçonnées sont mises en lien avec les premiers éléments de l'enquête afin d'ajouter certaines personnes à leur liste de suspect.es. Quasi systématiquement, pour chaque suspect.e, ils récupèrent ses 5 contacts les plus réguliers, demandent leurs fadettes et selon l'activité téléphonique qu'ils observent (notamment le jour des faits reprochés), ils décident ou non d'ajouter de nouvelles personnes à leur liste de suspect.e.s.

Enfin, grâce à la surveillance et à l'étude de diverses données et informations, la police a cherché à étoffer les dossiers des personnes suspectées pour y ajouter tout ce qui pourrait être utilisé comme indice ou qui pourrait créer des liens entre les personnes et ainsi démontrer la constitution d'une "bande organisée".

[4] Ces logiciels espions sont développés et installés par le service technique national de captation judiciaire (STNCJ), un service de la DGSI.

[5] Protonmail a par exemple déjà donné dans le cadre d'une enquête l'adresse IP qui a servi à la création d'un compte

[6] Notons aussi que d'autres dossiers d'enquête récents (sur les manifestations de Sainte-Soline ou encore la note des renseignements sur les Soulèvements de la terre) montrent des informations et/ou photos probablement issues de la présence de policier.es en civil lors de campements, rassemblements et manifestations publiques.

[7] Par défaut, la mémoire des iPhones est chiffrée. Pour la déchiffrer, il faut deux clés : l'une est dérivée du mot de passe de l'utilisateur.ice (souvent un mot de passe à 6 chiffres), l'autre est une clé inscrite physiquement dans les composants électroniques de l'iPhone, et conçue pour ne pas pouvoir être sortie de ceux-ci. La première possibilité pour un.e attaquant.e qui voudrait accéder à la mémoire serait de bruteforcer le mot de passe de l'iPhone directement sur celui-ci. Mais le système impose un délai entre deux essais, délai qui augmente au fil des échecs. Bruteforcer un mot de passe à 6 chiffres (ce qui ne prend pas longtemps d'habitude) devient alors plutôt interminable. L'autre possibilité qui s'offre est alors de procéder à une extraction physique de la mémoire de l'iPhone, et de bruteforcer celle-ci. Mais il leur faudra alors trouver et le mot de passe et la clé inscrite physiquement dans les composants électroniques. Et celle-ci est très longue, la bruteforce devient donc très longue elle aussi. Cellebrite, entreprise qui équipe les forces de l'ordre française en outils d'analyse forensiques, revendique pouvoir accéder aux données de n'importe quel iPhone, même à jour, et même récupéré éteint. Mais dans ce cas de figure, elle demande aux forces de l'ordre de leur fournir directement l'appareil et monnaient assez cher ce service.

[8] La police utilise l'appareil UFED de Cellebrite (entreprise de cybersécurité), un "aspirateur" à données qui liste les failles de sécurité de tous les modèles de téléphone et de tous les systèmes d'exploitation utilisés. C'est l'utilisation de l'UFED qui leur permet de contourner les systèmes de chiffrement des téléphones récupérés allumés mais l'UFED propose aussi les solutions de bruteforce d'extractions physique ou de bruteforce directement sur le téléphone. Seuls des services spécialisés utilisent l'UFED : pour les GAV à la SDAT, c'est la Sous-Direction de Lutte contre la Cybercriminalité (SDLC) qui est mobilisée ; quand les GAV sont menées par les gendarmes, c'est soit le Centre National d'Analyse Numérique qui est à Cergy, soit les sections opérationelles de lutte contre les cybermenaces qui sont départementales qui font les analyses. Une fois le contenu des mémoires des téléphones rendues lisibles, ces données sont transmises aux services d'enquête (SDAT ou SR), dans un fichier où les données sont triées par catégories (SMS, messages de messagerie chiffrées, photos, vidéos, enregistrements audios, …).

[9] Notons à ce sujet que, en France, des chantages en vue d'obtenir des informations régulières sur des ZADs, squats, mouvements écologistes, antifascistes, etc, en l'échange de supposée clémence ou de rétributions financières, ont été faits régulièrement en GAV ou dans d'autres cadres. De manière d'autant plus abjecte, des chantages aux papiers ont été régulièrement faits ces dernières années sur des personnes exilées lors de rendez-vous en préfecture ou dans des lieux publics pour leur faire comprendre qu'elles devraient donner des informations régulières sur des groupes et personnes qu'elles pouvaient côtoyer et obtenir ainsi des papiers ou être au contraire expulsées.

[10] Pour une explication du fonctionnement des VPN, il est possible de se reporter au guide Comment se protéger et protéger nos luttes, premiers pas dans la mise en place de pratiques de sécurité

[11] https://secoursrouge.org/android-possibilite-de-protection-contre-les-imsi-catcher/

confiance et intégrer des réflexes qui protègent à la fois les personnes et les capacités d'agir. Ces réflexes ne représentent pas forcément des efforts démesurés ! Passer par Signal plutôt que par les SMS, éviter les commérages et la curiosité déplacée sur qui a fait quoi, prendre l'habitude de communiquer des informations sensibles uniquement aux personnes qui en ont besoin…

Sans tomber dans le fantasme d'une surveillance permanente et omniprésente, autant prendre un certain nombre de mesures pour se protéger du traçage policier, tout en veillant à ce que ça ne nous pourrisse pas trop la vie et que ça ne nous empêche pas de nous organiser collectivement.

Nous travaillons à une analyse plus poussée de ces premiers éléments et d'autres. Vous pouvez nous contacter à lesmoyens@systemli.org

Notes

[1] La précision de la localisation issue des fadettes dépend de la densité des antennes relais aux alentours. En zone rurale, il est fréquent de n'avoir qu'une antenne tous les 10-20 km, donc avoir été connecté à cette antenne nous place dans un cercle de la moitié de cette distance. En zone urbaine très dense, il arrive d'avoir des antennes du même opérateur à 100 m l'une de l'autre, permettant ainsi une beaucoup plus grande précision sur les déplacements.
Comparer les antennes déclenchées entre plusieurs numéros, et en conclure que des personnes sont probablement souvent ensemble : "ces deux personnes ont déclenché tant de fois les mêmes antennes relais différentes aux même périodes temporelles". De même, ce genre d'informations est tiré d'un traitement automatisé des fadettes. Le logiciel utilisé n'est accessible qu'aux services enquêteurs.

[2] Cette géolocalisation n'est pas basée sur le GPS. Techniquement, des SMS silencieux sont envoyés au numéro pour générer du trafic de manière régulière (par exemple toutes les quelques minutes), le téléphone va se connecter à différentes antennes relais et la puissance du signal va être mesurée à chacune des antennes relais, permettant d'avoir une approximation de la distance à celle-ci. En triangulant ces informations, cela permet d'avoir une position beaucoup plus précise que seule l'info de l'antenne relais à travers laquelle transite la communication comme ce que conservent les fadettes. Cette localisation est transmise aux policier.es automatiquement et en direct, contrairement aux fadettes qui ne concernent que le trafic passé. La précision peut aller de quelques mètres dans une zone urbaine très dense à plusieurs centaines de mètres en zone rurale. La géolocalisation en direct ne permet pas toujours à la police d'intercepter physiquement des personnes, plusieurs exemples récents le montrent.

[3] Aujourd'hui, tout le trafic web étant chiffré sur le transit avec TLS (le httpS), il n'est pas possible de connaître ni le contenu consulté, ni même la page exacte vue. Seul le nom de domaine est visible : google.com, signal.org, wikipedia.fr ou caf.fr. C'est utilisé pour savoir s'il y a du trafic WhatsApp, Signal et dater ce trafic. Cela pourrait être également utilisé pour connaître l'heure de l'envoi d'un mail ou la connexion et faire des corrélations entre plusieurs personnes par ce biais (même si ça n'a a priori pas été utilisé dans l'enquête).

Avant les arrestations, mais sans que cela soit systématique, ils semblent avoir procédé à des filatures, probablement pour confirmer les domiciles des personnes surveillées.

1. Moyens d'enquête à partir de données récoltées sur place

1.1. Recherche d'ADN et d'empreintes digitales

La garde nationale a effectué des recherches dans la forêt et la garrigue dans un périmètre très large autour de l'usine et des objets divers et variés sur lesquels se trouve de l'ADN ont été récupérés. Certains, selon les policiers, ont "matché" avec des ADN déjà inscrits au FNAEG (Fichier National Automatisé des Empreintes Génétiques). Les ADN et empreintes digitales ont été retrouvés sur un objet calciné ou un emballage plastique.

La présence d'un ADN a par ailleurs permis aux enquêteurs de placer une personne en garde-à-vue, qui a été par la suite écartée du dossier.

Quant aux ADN qui n'ont pas "matché", ceux-ci ont étés inscrits au FNAEG sans être reliés à une identité. Si, plus tard, quelqun.e donne un ADN similaire à un de ceux enregistrés, son identité sera rattachée à l'enquête.

L'ADN est par nature mobile et non daté c'est-à-dire qu'aucun expert ne serait en capacité de dire si il était présent depuis un jour, dix jours, un mois, s'il résulte d'un contact direct entre le donneur ou l'objet ou s'il s'agit d'un transfert et enfin si l'objet a été transporté par la personne dont l'ADN a été retrouvé ou un tiers.

1.2. Demande d'images de vidéosurveillance

Immédiatement après le 10 décembre, les policier.es ont réquisitionné des images prises par les caméras de transport en commun (bus, gares…), de commerces, de caméras de surveillance de maisons privées ou de caméras de ville et ce dans un périmètre étendu autour du site Lafarge de Bouc-Bel-Air. Les images de vidéosurveillance n'étant pas généralement conservées au delà de deux semaines, on suppose que les policier.es ont du récupérer un maximum d'images dans un temps restreint. Ils ont commencé par demander et analyser les images de vidéosurveillance proches du site et étendu les demandes de vidéos le long des trajets selon eux pris par des personnes qui auraient pu avoir participé à l'action. Les policiers ont récolté, dès les premières semaines d'enquête, plusieurs centaines d'heures de vidéo dont l'exploitation a demandé plusieurs mois d'analyse.

Comme bien souvent pour les images issues de caméras de vidéosurveillance, il convient de noter que les images présentées au cours des gardes à vue sont de piètre qualité.

1.3. Reconnaissance faciale

Des images de personnes présentes dans des bus ou dans une zone à une proximité toute relative du site et qui ont été considérées comme suspectes, ont été comparés par un logiciel de reconnaissance faciale avec le fichier du TAJ (Traitement d'Antécédents Judiciaires) qui contient les photos de signalétique prises durant les GAV.

Les policier.es ont également repéré les habits et les sacs portés par les personnes qu'iels suspectent et pensent reconnaître sur des images de vidéosurveillance. Lors des perquisitions, iels ont essayé de trouver des vêtements/accessoires similaires.

Les policier.es de la section de recherche de Marseille ont aussi demandé aux opérateurs téléphoniques les données de téléphonie ayant transité par les antennes relais à proximité du site Lafarge, afin d'identifier les personnes présentes sur les lieux et donc d'éventuel. les suspect.es. On y reviendra ci-dessous dans la partie 2.2. Bornage à certaines antennes relais.

2. Moyens d'enquête liés à la téléphonie

Une immense partie de cette enquête repose sur la téléphonie. Les enquêteur.ices se basent sur l'analyse des contacts et de l'activité du téléphone (bornage) pour fabriquer des profils suspects.

Pour établir ces liens, iels passent parfois par l'analyse de l'activité téléphonique de personnes totalement hors de cause, d'où l'importance d'avoir des pratiques communes de protection de sa vie privée. Les différents moyens sont classés des plus utilisés (fadettes) aux plus rares (géolocalisation) jusqu'aux plus exceptionnels (logiciel espion).

Ces analyses ne prennent en compte aucun facteur humain, le prêt de son téléphone, son oubli et techniquement tout ce qui relève du délestage, c'est-à-dire quand une antenne est amenée à gérer un flux trop important, et qu'elle mobilise une autre antenne.

2.1. Étude des fadettes (factures détaillées)

Les fadettes sont quasi systématiquement demandées lorsqu'un numéro porte un intérêt dans une enquête, c'est vraiment un outil de

bon de se poser la question : ces outils/techniques protègent-ils bien ? Sont-ils réalistes à mettre en œuvre ?

Conseils pour la garde-à-vue

Évidemment, le mieux, c'est de garder le silence pour toutes les questions, même les plus basiques, de ne rien signer, et de refuser la signalétique (empreintes et photos), et la prise d'ADN, dans la mesure du possible.

Pour les personnes ayant déjà fait une GAV et qui ont déjà donné leur signalétique (empreintes digitales et photos) et/ou leur ADN, et pour éviter que ceux-ci ne matchent dans le futur avec des images de vidéosurveillance, des empreintes ou de l'ADN retrouvés sur un lieu d'action ou tout simplement pour protéger au mieux ses données, il est parfois possible de les faire effacer des fichiers de la police. Il faut demander à avoir accès aux fichiers du TAJ (Traitement des Antécédents Judiciaires), FAED (Fichier Automatisé des Empreintes Digitales) et FNAEG (Fichier National Automatisé des Empreintes Génétiques) nous concernant puis l'effacement de ces données. C'est une démarche un peu longue et qui coûte cher en recommandés mais on se dit que ça peut valoir le coup (voir le guide “La folle volonté de tout contrôler” dans les ressources).

Conclusion

En terme de sécurité, on peut être tenté.es de rapidement baisser les bras et partir du principe que la police sait déjà beaucoup de choses, et que ça ne sert à rien de mettre en place telle ou telle pratique de sécurité.

Les enquêtes en cours ou achevées montrent que les policier.es, même l'élite de la police judiciaire, ne savent pas tout, se trompent, mais sont en mesure de passer des mois ou de mobiliser des dizaines de personnes pour analyser de grosses quantités de données. Ce sont avec des moyens d'enquêtes classiques (analyse de vidéosurveillance, analyse des fadettes), que les services de polices alimentent le plus leur dossier. Les policier.es ont dressé une première liste de suspects avec ces moyens d'enquêtes, puis ont soupçonné des contacts et/ou contacts de contacts. En général beaucoup des erreurs et maladresses qui les amènent à soupçonner des gens peuvent etre corrigées. Les moyens très poussés que les policier.e.s ont voulu utiliser (sonorisation, logiciels espions), semblent encore assez complexes à mettre en place pour elleux.

Il nous semble important de réussir à mettre en œuvre des pratiques de sécurité communes. Développer une culture de sécurité commune, c'est se donner les moyens d'appréhender les risques, construire de la

même s'ils sont sécurisés, n'offrent pas une protection absolue. Sur Signal, il est bon de ne pas partager des informations trop sensibles.

- Dans Signal, mettre les messages éphémères par défaut : paramètres → confidentialité → messages éphémères. 1 jour ou pas beaucoup plus, quitte à régler ensuite et rallonger suivant les conversations..
- Ne pas avoir de noms de groupes trop explicites. Ex : braquage n'est pas vraiment une très bonne idée de nom de groupe.
- Avoir suffisamment de personnes administratrices dans chaque groupe pour éviter que, par malchance, la seule personne administratrice soit arrêtée avec son téléphone.
- Quand une personne présente sur une boucle signal est mise en GAV et son téléphone saisi, il faudrait au plus vite supprimer son numéro de toutes les boucles signal sur lesquelles elle est.
- S'il y a un doute sur des arrestations massives de personnes sur un groupe, il est possible de recréer une nouvelle boucle uniquement avec les personnes dont on peut s'assurer qu'elles sont encore libres.
- Malgré la suppression d'une personne d'une boucle Signal, il est toujours possible de voir depuis son téléphone (si elle n'a pas elle-même supprimé la conversation), les membres de la boucle au moment où la personne a été supprimée, ainsi que les messages non-effacés.
- Ne pas synchroniser les contacts du téléphone avec Signal.
- À la configuration de Signal, il est possible de donner n'importe quel numéro de téléphone qui puisse recevoir le code de vérification. Ainsi cela permet d'avoir un compte Signal qui ne soit pas relié à un état-civil.

Conseils pour les ordinateurs [d'infos dans la brochure TuTORiel Tails et dans le Guide d'auto-défense numérique]

- On recommande fortement l'utilisation de Tails pour les activités militantes, et de ne pas laisser traîner son ordinateur et sa clé tails sans surveillance de manière à éviter que des personnes mal intentionnées puissent y avoir accès.
- Pour ses activités militantes, utiliser le navigateur Tor Browser autant que possible.
- Toujours effacer les méta-données de tout document voué à la publication. Sous Tails, un clic-droit sur un fichier permet de choisir "effacer les méta-données". Signal, lui, le fait automatiquement quand à l'envoi d'un fichier, excepté la date de prise de bue souvent présente dans le nom du fichier.
- Pour augmenter la sécurité des échanges par e-mail, utiliser des instances mails comme Riseup, Disroot, Systemli ou Immerda. Il est bon de chiffrer ses mails avec le protocole openPGP (voir les guides précités).
- Chaque contexte exige des choix de sécurité différents. Il est ncéssaire de se poser les questions : qu'est-ce que je veux protéger et contre qui ? Une fois ces questions posées, on peut choisir des techniques et outils pour y apporter une réponse. Une fois ceci fait, il est

récupération très large d'informations. Étant vues comme peu intrusives en terme de vie privée, leur demande n'a pas besoin d'être validée en amont par un magistrat, elle se fait par une plateforme automatisée en lien avec les opérateurs, la plateforme nationale des interceptions judiciaires (PNIJ). Les résultats sont obtenus en quelques minutes et coûtent quelques euros par numéro. Nos entretiens nous ont permis de penser que les fadettes de plus d'une centaine de numéros ont été demandées dans le cadre de l'affaire Lafarge.

Pour communiquer sur le réseau, un téléphone a besoin de se connecter à des antennes. Pour ce faire, il communique systématiquement deux informations : son IMEI, qui identifie la puce GSM, et le numéro de la carte SIM (numéro IMSI). Les fadettes sont un tableau comprenant les données suivantes :

l'IMEI du "boîtier" : le numéro unique de la puce qui permet la communication des données sur le téléphone, qui permet d'en déduire le modèle. Si votre téléphone a 2 slots SIM, il a deux numéros IMEI qui ne sont a priori pas faciles à lier.

- Le moyen de communication (SMS, appel, DATA)
- Le jour et l'heure
- L'antenne relais par laquelle passe ce trafic
- Le numéro de l'autre correspondant·e et le sens du trafic (sortant ou entrant)
- La durée de l'appel ou la taille du SMS

À moins d'être mis.e sous écoute ou qu'un logiciel espion ait été installé sur le téléphone, il n'est pas possible de connaître le contenu des appels/SMS ni du trafic internet.

Les fadettes sont conservées pendant 1 an par l'opérateur téléphonique, les policier.es peuvent donc avoir accès aux données des 12 mois précédant leur demande. Une fois demandées pour un numéro, les fadettes peuvent être conservées dans le fichier Anacrim de recoupement des enquêtes judiciaires. De futures enquêtes peuvent donc avoir accès à des fadettes ayant plus de 12 mois.
Les fadettes sont utilisées pour :

- Analyser la répartition entre le trafic DATA et SMS/appels ce qui permet de déduire l'utilisation majoritairement de messageries passant par internet par exemple.
- Faire des réseaux de liens entre des personnes qui échangent par SMS/appels, par exemple supposer que deux personnes se connaissent car elles sont en contact avec la même personne (ces traitements sont facilités par le logiciel Analyst Notebook / Anacrim).
- Suivre les déplacements des personnes grâce aux très fréquentes communications DATA d'un smartphone. Selon les antennes déclenchées ("le bornage") on peut déduire un déplacement en train, ou en voiture,

selon les arrêts on peut déduire que la personne fait du stop. [1]

Ils reçoivent donc une liste des communications téléphoniques (SMS, MMS, appels, données mobiles), et, comme pour les fadettes, leurs émetteurs, leurs receveurs, les numéros IMEI utilisés. La quantité de données est beaucoup trop importante pour essayer d'identifier chacun.e des personnes présentes aux alentours. Les gendarmes comparent même une liste de numéros de personnes ayant fréquenté la ZAP de Pertuis à la liste des numéros ayant borné à proximité du site. Ensuite, iels demandent les fadettes des personnes ayant fréquenté la ZAP de Pertuis, par lesquelles iels obtiennent les contacts de ces personnes, et comparent la liste de la ZAP et de leurs contacts avec celle des téléphones ayant communiqué avec les antennes relais présentes autour des lieux du site Lafarge.

2.2. Réquisition des évènements réseaux

Les policier.es peuvent demander la liste de toutes les communications passées via une antenne relais entre deux dates. À Bouc-Bel-Air, iels demandent l'entièreté du trafic passé sur les antennes relais proches du site Lafarge entre 12h et 20h le 10 décembre.

Un téléphone, même quand il n'émet ni ne reçoit de communication téléphonique (SMS, MMS, appels, données mobiles), échange très régulièrement des informations avec les antennes relais à proximité, notamment pour que le réseau sache où envoyer les éventuelles communications que le téléphone pourra recevoir (ces échanges d'informations permettent par exemple au téléphone d'afficher un niveau de réseau, qui s'affiche en haut à droite ou à gauche de l'écran). Ces données ne sont pas des "communications téléphoniques" à proprement parler, elles n'aparaissent donc pas sur les fadettes, et les opérateurs les appellent "évènements réseaux. Les évènements réseaux permettent d'obtenir des informations bien plus fines que les fadettes : si plusieurs minutes ou heures peuvent séparer deux communications, deux lignes, dans les fadettes, moins d'une minute sépare chaque échange des "évènements réseaux". Les services enquêteurs peuvent donc savoir à peu près à la seconde près la présence d'une personne dans l'espace couvert par une antenne relais, et le déplacement vers une autre antenne. Une présence de quelques secondes dans cet espace, ou même une présence longue mais sans qu'il n'y ait de communication seront donc remarquées avec les "évènements réseaux" et ne le seront pas avec les fadettes. Pour obtenir les "évènements réseaux", les policier.es se déplacent sur place et prennent des mesures pour savoir, pour chacun des 4 principaux opérateurs, quelles antennes relais couvrent le lieu, avant de les réquisitionner pour les obtenir. Free n'enregiste pas (ou ne communique pas) ses évènements réseaux. Au même titre que les des majuscules et minuscules] Le coût pour casser un tel mot de passe peut s'avérer gigantesque tant en énergie qu'en matériel et prendrait actuellement plusieurs années en mobilisant une puissance de calcul astronomique.

Pour éviter d'avoir une activité téléphonique trop facile à analyser :

- Éviter de prendre son téléphone avec soi (en action, en manif, en réunion, en rassemblement ou autre). Cependant, le laisser chez soi sans activité peut être considéré par la police comme un comportement suspect, on l'a vu. On peut toutefois imaginer que d'autres personnes puissent se servir d'un téléphone. On peut aussi mettre son téléphone régulièrement (quelques heures ou quelques jours) en mode avion, afin que l'absence d'activité soit un comportement habituel dans l'usage de notre téléphone.
- Éviter au maximum les appels téléphoniques en clair et les SMS.
- Utiliser au maximum le Wifi. Cela réduit grandement le trafic 4G rendant plus difficile l'exploitation des habitudes d'utilisation du téléphone.
- Utiliser un VPN permanent sur le téléphone pour compliquer, lors d'éventuelles interceptions, l'analyse des données mobiles [10].
- Si on se fait arrêter et que notre téléphone est saisi, on peut bloquer puis refaire sa carte SIM dès sa sortie de GAV. Puis réinstaller Signal sur un nouveau téléphone. Cela désactivera la carte SIM et le Signal qui sont restés au commissariat. Les nouveaux messages reçus ne pourront pas être lus.
- Si on utilise un dumbphone anonyme, pour éviter que celui-ci puisse être associé à un éventuel appareil non anonyme, il vaut mieux ne pas les utiliser en même temps et au même endroit car la connexion répétée aux mêmes antennes pourrait les lier de fait.
- Il est possible d'acheter une carte SIM dans un bureau de tabac sans donner son identité. Par exemple si Lycamobile demande d'enregistrer son identité au bout d'un mois, le contrôle qu'ils ont l'obligation d'exercer s'avère lacunaire. De même, on trouve dans n'importe quel supermarché des dumbphones pour moins de 20€.
- Dans les fadettes, le numéro IMSI (numéro de carte SIM) et numéro IMEI (numéro associé au téléphone) sont associés. Si on veut changer de carte SIM, mieux vaut aussi changer de téléphone, et inversement, sinon les deux seront automatiquement reliés.
- Les IMSI-Catcher peuvent exploiter le réseau 2G pour collecter des informations. Sur Android, il est possible d'interdire le passage par le réseau 2G, en décochant l'option dans Paramètres → Réseau et Internet → SIMs → Autoriser 2G [11].

Signal

L'application et le protocole qui protège les communications sur Signal,

récemment, dirigés sur une personne du mouvement anti-bassines ou des lieux collectif comme les Tanneries ou les Lentillères à Dijon, sans que cela semble correspondre pour le moment à une enquête. On peut supposer qu'il s'agit de renseignement.

Il n'y a pas de trace à ce stade d'introduction de logiciels espions dans des ordinateurs. Cela avait été utilisé dans le cadre de l'affaire du 8/12 ou de la Creuse.

Quelques réponses : pratiques à adopter

Dans le cadre de ce texte, nous allons nous centrer sur quelques pratiques faciles à mettre en œuvre et applicables rapidement. Nous avons listé des pratiques ci-dessous classées en plusieurs catégories : smartphones, Signal, ordinateurs et garde-à-vue. Un certain nombre de guides plus complets existent et sont listés à la fin du texte. Nous vous conseillons vivement de les consulter.

De manière générale, en terme de sécurité, on peut être tenté.e.s de rapidement baisser les bras et partir du principe que la police sait déjà tellement de choses que ça ne sert à rien de mettre en place telle ou telle pratique de sécurité. L'enjeu policier étant de créer des réseaux de malfaiteur.euses, même si des liens entre des personnes semblent simples à faire (parce qu'elles vivent ensemble ou qu'elles se connaissent depuis longtemps), il est quand même toujours préférable de ne pas s'appeler en clair ou de ne pas se faire de virements bancaires, pour ne pas rajouter d'éléments. Il est toujours possible de réduire les risques en protégeant sa vie privée et politique.

Smartphones

Les smartphones sont des cibles de choix pour les enquêteur·ices.

- Un téléphone récent et mis à jour constitue une meilleure protection contre les tentatives d'accéder à son contenu. On peut prendre comme habitude d'éteindre son téléphone régulièrement et d'installer les mises à jour.
- Chiffrer son téléphone et définir un mot de passe suffisant pour protéger des attaques par force brute. L'attaque par force brute consiste à tester, une à une, toutes les combinaisons possibles. Un code à 18 chiffres parfaitement aléatoires ou un mot de passe de plus de 10 caractères avec lettres minuscule et majuscule parfaitement aléatoires sont considérés comme “sûrs”. [Pour que ce soit plus simple à retenir, on peut utiliser comme mot de passe plusieurs mots à la suite, en intercalant des chiffres, caractères spéciaux, et en utilisant

fadettes, les évènements réseaux sont accessibles pendant 1 an.

2.3. Géolocalisation en direct

Ce dispositif d'enquête doit être motivé par les enquêteur·ice·s, puis validé par un.e magistrat.e. Les téléphones attribués à une vingtaine de personnes visées dans l'affaire “Lafarge” ont étés géolocalisés en temps réel. Les données récoltées ne font pas forcément l'objet d'une analyse de la part de services d'enquête, laissant penser que cette mesure est parfois prise dans le cadre de la phase d'interpellation pour être sûr.es de savoir où sont les personnes soupçonnées quand vient le moment de les arrêter [2].

2.4. Utilisation d'IMSI catchers

Techniquement, un IMSI catcher est un appareil qui se fait passer pour une antenne relais dans l'objectif de capter les numéros de téléphone qui communiquent dans le rayon d'action de celui-ci. Il peut aussi être utilisé pour intercepter les communications, mais ça n'a, de ce qu'on sache, pas été le cas dans l'enquête. Les plus petits rentrent dans une valise.

Des IMSI catchers ont été utilisés dans le cadre de l'enquête. Dans un des cas, on suppose que l'IMSI catcher est utilisé pour chercher si la personne espionnée utilise une deuxième ligne téléphonique. Pour ce faire, iels procèdent avec l'IMSI catcher à une filature de la personne, et relèvent à plusieurs reprises l'ensemble des lignes téléphoniques qui communiquent proches de celle-ci. Iels obtiennent donc plusieurs listes prises à des endroits géographiquement différents. Les numéros de téléphone qui se retrouvent sur toutes les listes bougent avec la personne surveillée et il est possible de supposer que ce sont les numéros qu'elle utilise. Dans les autres cas, les IMSI catchers semblent avoir été mobilisés pour confirmer ou affiner la domiciliation d'une personne. Ils supposent que la personne vit à une adresse, mais elle pourrait vivre à une autre adresse couverte par la même antenne relais, et utilisent donc un IMSI catcher (qui, dans la plupart des cas, a un rayon d'action bien inférieur à celui d'une vraie antenne relais) qu'iels activent devant le domicile de la personne surveillée pour confirmer son adresse.

2.5. Interceptions téléphoniques (“écoutes”)

Ce dispositif d'enquête doit être motivé par les enquêteur·ice·s, puis validé par un magistrat. A priori, seuls certains des numéros des personnes mises en cause dans l'affaire à un moment donné ont eu une demande d'interception. Ces interceptions permettent d'accéder au contenu des communications SMS, appels téléphoniques en clair et au trafic DATA. Les appels sont enregistrés pour une retranscription

manuelle future, mais également retransmis en direct sur une ligne spéciale d'un.e chargé.e de l'enquête, leur permettant d'avoir un suivi très efficace.

L'interception permet également d'avoir le détail du "trafic internet" : avoir un horodatage des sites consultés, ou de tout serveur avec lequel une application communique [3].

L'utilisation d'un VPN de manière permanente sur un téléphone (et sur un ordinateur lorsque l'on utilise pas Tails) permet de se prémunir de l'analyse du trafic internet lors d'une interception téléphonique.

2.6. Introduction de logiciels espion (nommés "keylogger" dans l'enquête)

Après avoir demandé une interception ou une écoute, l'analyse du trafic internet a pu indiquer l'utilisation prépondérante de Signal comme moyen de communication. La juge d'instruction a demandé dans certains cas l'installation d'un logiciel espion sur des téléphones. La demande d'installation est à priori encore très rare et peu de traces de techniques similaires sont présentes dans la presse.

Ces dispositifs ont pour objectif d'avoir accès au stockage des données du téléphone, à ce qui est tapé et apparaît à l'écran et aux conversations chiffrées de type Signal. Dans cette enquête, à priori au moins cinq demandes d'installation à distance de logiciels espion ont été faites, mais, dans ce qui apparaît à ce stade dans le dossier, une seule installation a été fructueuse (sur un iPhone SE 2020).

Celle-ci pourrait avoir été réalisée par un accès physique au téléphone. Elle a permis, de manière certaine, d'avoir accès à une conversation de groupe Signal. Le contenu de la conversation et les participant·e·s seraient ainsi connues des enquêteur·ice·s.

Ce numéro ayant été inscrit à d'autres boucles Signal, il est fort probable que les enquêteur·ice·s aient aussi eu accès à ces autres boucles [4].

3. Demandes d'informations diverses

3.1. Réquisitions diverses pour collecter des informations larges sur les personnes visées par l'enquête

Des réquisitions ont été faites à la CAF, Pôle emploi, les impôts… ce qui permet d'obtenir entre autres des adresses de domicile et des numéros de téléphone, ainsi que des informations sur la situation personnelle des personnes suspectées. Ces réquisitions sont faites :

récupéré éteint n'a pas pu être déchiffré, alors même que les policier. es ont tenté de bruteforcer pendant 2 jours l'extraction physique qu'iels avaient réalisé de la mémoire de l'iPhone [7].

Un téléphone à jour et avec un mot de passe/code pin d'une longueur suffisante permet de réduire fortement les risques de déverrouillage des téléphones (voir les conseils en deuxième partie) [8].

5.3. Prise des ADN

Pendant les arrestations, les policier.es ont insisté pour que les personnes arrêtées portent des masques chirurgicaux pendant le transport, pour leur propre bien. Ces masques ont ensuite été mis sous scellés puis transmis aux services de police scientifique. De plus, pendant les perquisitions, des brosses à dents, des brosses à cheveux ou sous-vêtements ont été mis sous scellés. Les sous-vêtements portés par une personne ayant refusé de porter un masque pendant son transport ont étés saisis au cours de la GAV.

À la fin de sa garde-à-vue, les services de polices ont proposé à une personne de devenir indic contre rémunération. La personne a évidemment refusé et n'a pas pu savoir quelle somme d'argent ni quels étaient les objectifs de surveillance [9].

Moyens d'enquête qui n'apparaissent pas à ce stade dans le dossier mais qui existent légalement

Nous souhaitions rapidement mentionner certains moyens d'enquêtes qui n'apparaissent pas pour le moment, mais qui sont légaux et qu'on sait utilisés parfois par des services d'enquête comme la SDAT ou la DGSI. En effe, l'ouverture d'une instruction judiciaire signifie surtout un nouveau cadre d'enquête après la flagrance et l'enquête préliminaire, donc l'enquête continue.

Il n'y a pas d'élèment à ce stade du recours d'informations obtenues par des policièr·e·s infiltré·e·s ou des indics.

Il n'y a pas de trace non plus de sonorisation d'habitation ou de jardin. Mais cela a été utilisé dans le cadre d'une enquête judiciaire sur un incendie d'antenne relais dans la Creuse. C'est aussi une technique de renseignement, un micro a par exemple été découvert à l'intérieur d'une photocopieuse dans la librairie anarchiste Libertad à Paris.
Pour une recension de ces découvertes, y compris à l'échelle européenne : https://www.csrc.link/earsandeyes/fr/

Il n'y a pas de trace à ce stade de caméras cachées devant ou à l'intérieur des habitations. Mais de tels procédés sont apparus

5.2. Accès au contenu des téléphones pendant et après les GAV

Certains smartphones ont pu être déchiffrés par la Sous-direction antiterroriste (SDAT) ou d'autres corps de police pendant le temps des GAV. D'autres ont résisté aux opérations de forçage menées pendant les GAV, mais vont probablement continuer à subir des tentatives plus poussées avec d'autres outils par la suite.

Dans les cas où les enquêteurs ont pu avoir accès au contenu de téléphones et que ceux-cis étaient sur des groupes Signal comportant un grand nombre de membres, ils ont donc eu accès à l'ensemble des numéros présents sur ces boucles ainsi qu'aux messages éphémères encore non effacés au moment de la prise des téléphones.

Dans les cas où le numéro Signal est lié à une ligne téléphonique personnelle elle même liée à une identité civile, cela permet directement aux enquêteur.ices d'identifier à qui appartient le numéro. Cette personne sera éventuellement fichée.

Dans le cas ou le numéro Signal est lié à une carte SIM ou un numéro plus anonyme, cela leur donne un numéro à inscrire dans un fichier sans renvoyer à une personne identifiable. Cependant, les enquêteur.ices peuvent tenter d'identifier un numéro par son pseudo Signal, par des contenus de messages éphémères pas encore effacés au moment de la saisie ou par l'activité de la carte SIM (SMS, appels en clairs et bornage à domicile).

La police a eu accès aux données chiffrées de certains smartphones allumés en utilisant les failles de sécurité qui existent lorsque le téléphone est allumé. Elle a aussi, pour les téléphones récupérés éteints, tenté de bruteforcer le mot de passe (enchaîner tous les mots de passe possibles jusqu'à trouver le bon). Il est possible de le faire depuis le téléphone, mais souvent le système impose un délai entre deux tentatives, ce qui rend la technique extrêmement coûteuse en temps. Pour contourner ce problème, les policier.es peuvent extraire la partition chiffrée afin de tenter de la forcer depuis un ordinateur. La possibilité de réaliser l'une ou l'autre technique dépend de chaque smartphone.

Précisons que sur des téléphones Android récents, que le téléphone soit récupéré allumé ou éteint ne semble pas changer grand chose. Sur tous les Android, une extraction physique a pu être réalisée et a permis d'extraire la partition chiffrée et les clés, permettant de bruteforcer le code. Sur les iPhones exploités (le plus récent étant un iPhone SE 2020), le fait que le téléphone soit allumé a permis aux enquêteur.ices de contourner le dévérrouillage et de ne même pas avoir besoin de bruteforcer le mot de passe. Un iPhone SE 1e génération (2016)

- À des administrations publiques comme l'ANTS (Agence Nationale des Titres Sécurisés) pour obtenir les photos d'identité. Lorsqu'une personne apparaît comme suspecte, par exemple parce qu'elle est un contact téléphonique régulier d'une autre personne soi-disant identifiée par reconnaissance faciale et parce que son propre téléphone apparaît inactif ou borne à proximité du lieu des faits le 10 décembre, les enquêteur.ices réquisitionnent les photos qui ont servi à la demande de documents d'identité, puis les comparent aux images de vidéo-surveillance.
- À des entreprises privées de déplacement comme Blablacar, la SNCF, FlixBus permettant d'obtenir des déplacements supposés (notons que Blablacar dispose d'un contact police dédié et divulgue l'ensemble des adresses IP utilisées pour réserver un voyage) ;
- À des banques afin d'examiner l'activité bancaire de suspect.es (des gens mais aussi des associations), pour récupérer les noms des émetteur.ices ou bénéficiaires de virements, interpréter des retraits, ou faire d'autres réquisitions à des sites de vente en ligne pour connaitre le détail d'achats ayant été faits via ce compte.
- À des réseaux sociaux, qui peuvent leur transmettre les adresses IP de connexion ou de création des comptes visés par l'enquête. Des comptes Twitter, Facebook et Instagram font l'objet de réquisitions, Facebook refuse de leur transmettre ces informations.

À noter que plusieurs des personnes visées par ces réquisitions ont vu leur compte en banque clôturé sans explication ou ont subit des contrôles domiciliaires très poussés par la CAF. Une clôture de compte bancaire inexpliquée peut ainsi être un signe de surveillance.

La police dit ne pas envoyer de réquisitions à Riseup par peur qu'iels ne préviennent les personnes concernées, et considérant que Riseup ne leur répondra probablement jamais. Cela semble confirmer que l'utilisation de fournisseurs mail militantes mettant en œuvre un certain nombre de protections et de système de chiffrement tels que Riseup leur pose beaucoup plus de problèmes d'accès que dans le cas de fournisseurs commerciaux [5]. (Il va sans dire que l'utilisation de clés de chiffrement PGP pour les échanges de mails ajoute une couche de protection supplémentaire).

3.2. Données issues des services de renseignements

On trouve mention d'informations venant de "services partenaires", expression qui parle de divers types de services de renseignements : DGSI, Renseignements Territoriaux (SCRT) ou les renseignements de la gendarmerie (SCRCGN). Certains noms semblent ainsi apparaitre dans le

dossier sans que l'on ne sache vraiment d'où les policiers les sortent et ont pu donner lieu à des questions lors des gardes-à-vue, en audition ou « en off ».

4. Dispositifs de surveillance

4.1. Demande de sonorisation d'au moins un véhicule.

Moyen d'enquête particulièrement intrusif, la sonorisation peut être effectuée après accord d'un juge, et peut être réalisée tant dans un véhicule qu'un domicile. Elle vise la captation des paroles mais il ne semble pas que l'opération ait pu être menée à bien jusque-ici.

4.2. Mise en place de boîtiers GPS sous des véhicules

Au moins 3 traceurs GPS ont été utilisés dans l'enquête. Une personne arrêtée a retrouvé sur sa voiture, après les GAV, un traceur non mentionné pour le moment dans le dossier. A priori, ces traceurs sont fabriqués par la société track-cars (connue pour vendre de tels dispositifs aux services de police français).

4.3. Filatures

Les policier.es ont suivi des personnes dans la rue, dans les transports en commun, dans leurs déplacements en voiture. Ces filatures sont utilisées à la fois pour identifier de nouvelle/aux suspect.es en cherchant les gens que fréquentent les personnes impliquées dans l'enquête, mais aussi souvent confirmer une identité ou pour "loger" un.e suspect.e (trouver l'adresse de qelqu'un.e dans le jargon policier), avant une perquisition.

Les policier.es commentent aussi des comportements lors de rassemblements publics. Exemple : untel ne parle pas à untel lors de tel rassemblement public alors que l'on considère par ailleurs qu'iels se connaissent. Iels font donc semblant de ne pas se connaître et cachent quelque chose [6].

4.4. Demande de photos des véhicules aux péages autoroutiers

Des réquisitions ont été faites aux sociétés d'autoroute pour avoir les photos de véhicules qui les intéressent au moment de passer le péage, pour pouvoir éventuellement identifier les passager.es.

Pour connaître le véhicule, ainsi que le.a conducteur.ice qui transporte une personne visée par l'enquête. La géolocalisation du téléphone, ou le paiement au péage, permet d'avoir une plage horaire très restreinte de photos à regarder.

Pour savoir quel.les sont les occupant.es de véhicules connus et utilisés pour aller à une manif, et vont faire des réquisitions pour obtenir des photos pour tenter d'identifier des passager.es de ces véhicules.

4.5. Renseignement en source ouverte

Évidemment, les policier.es cherchent sur internet pour trouver les textes, les posts sur les réseaux sociaux, les prises de paroles lors de conférences publiques de groupes qu'iels rapprochent de l'enquête, les informations personnelles sur les personnes recherchées. Iels analysent aussi les reportages télévisés sur l'invasion-sabotage du site Lafarge.

Différents textes critiques parus sur des sites militants sur les Soulèvements de la Terre semblent utilisés dans le dossier par les policier.es pour appuyer leur idée d'une séparation entre les "commanditaires" et les "exécutant.es", cela leur servant à projeter des rôles impliquant des culpabilités spécifiques pour certain.e.s des gardé.e.s à vue. Ces textes ont aussi été distribués à certain.e.s en garde-à-vue, peut être pour tenter, lors des auditions, de diviser les personnes mises en cause.

Dès le début de l'enquête, les policier.es analysent les photos de l'action contre Lafarge, publiées sur le site des Soulèvements de la Terre, qui contenaient des métadonnées comprenant un nom ainsi que le numéro de série d'un boîtier d'appareil photo. Ils ont demandé au constructeur de divulguer le nom de l'acheteur. Le constructeur a donné le nom du magasin où le boîtier a été vendu. La combinaison de ces deux données a permis en quelques jours d'identifier une personne, accusée d'avoir pris ces photos.

5. Moyens d'enquête liés aux arrestations

5.1. Perquisitions

Lors des perquisitions, les policier.es ont cherché à retrouver des vêtements et accessoires apparaissant sur les images de vidéosurveillance qu'iels ont utilisé pour reconnaître les personnes. Iels ont aussi cherché du matos numérique (ordinateurs, téléphones, clés USB, disques durs), des carnets et tout autre objet pouvant relier à l'action du 10 décembre. Aussi, iels ont pris des objets qui pouvaient contenir de l'ADN des personnes suspectées (brosse à dent, sous-vêtement…).